U.S. Department of Agriculture
Office of the Chief Information Officer
Cyber Security

IT Security Awareness
USDA New Employee Orientation

Revised August 2006

Orientation Introduction

1. Basic concepts for overall security awareness at USDA.
2. Good computer security practices for everyday use.

Learning Objectives

Explain the importance of security awareness as it relates to the Department as a whole and to you as an employee of the Department and a caretaker of a U.S. Government computer and USDA data.

1. Identify threats and vulnerabilities to information security at USDA and incorporate safeguards from threats and vulnerabilities into your daily routine.
2. Understand your roles and responsibilities as they relate to basic practices for computer security, including the use of computer assets, securing ID’s and passwords,and protecting all your information technology equipment.

Overall Security Awareness

Appropriate security measures *ensure the ability of the agency to achieve its mission*….

Whether it be providing economic opportunities for farmers….

Overall Security Awareness

Ensuring a safe food supply….

Overall Security Awareness

or caring for forests and range lands…

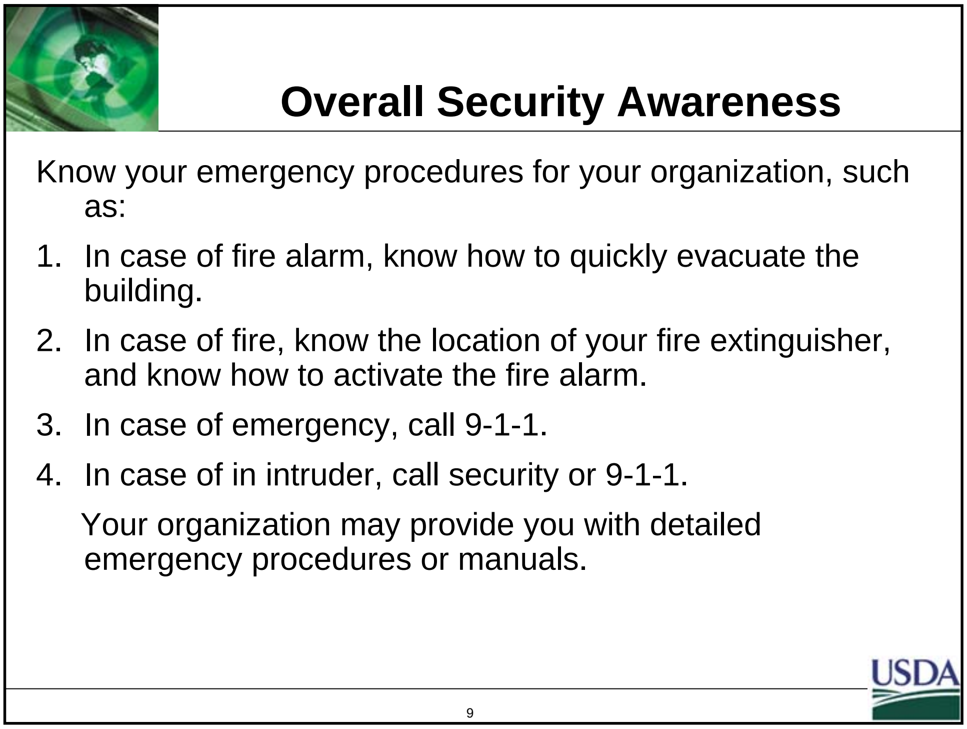
Overall Security Awareness

- The accomplishment of USDA mission depends on accurate available services and information systems that are protected from potential disclosure, tampering, and harm.
- Good security ensures the confidentiality, integrity, and availability of our information and systems so that we can fulfill our mandate of “enhancing the quality of life for the American people by supporting production of agriculture.”

Overall Security Awareness

Physical Security Awareness Practices….

1. Report any suspicious activities that you see. Examples include**:**
   - Unattended packages
   - Suspicious people
2. Access Control
   - Are your Entrance Doors guarded or locked?
   - Does your organization require ID Badges to be worn at all times?
   - Do you ask for identification if you meet a stranger in a secure area?

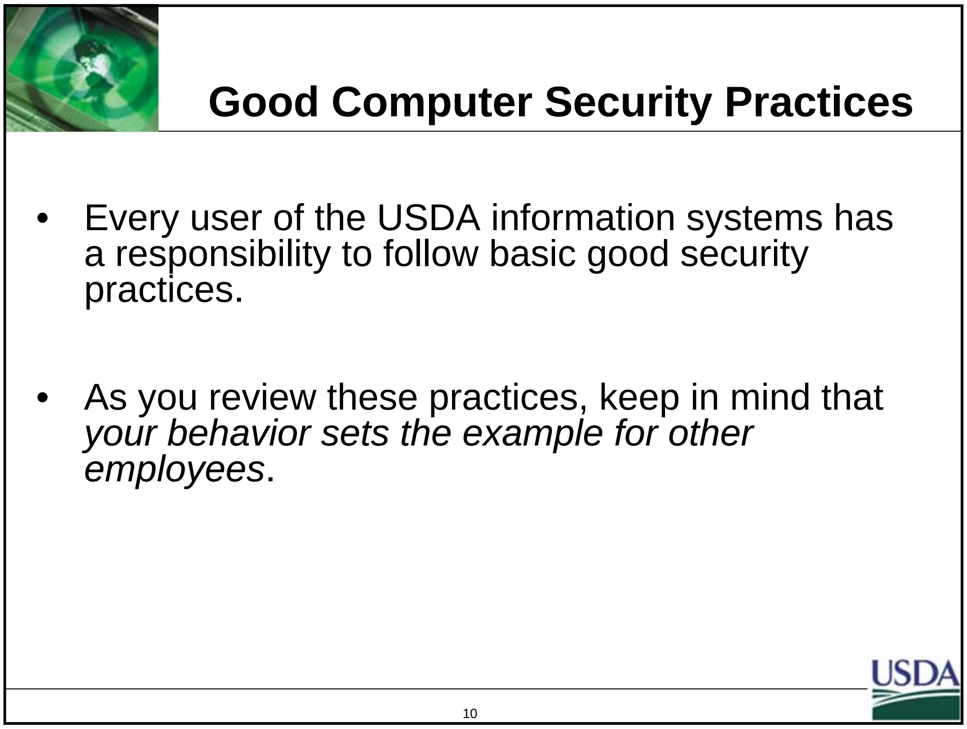


Overall Security Awareness

Know your emergency procedures for your organization, such as:

1. In case of fire alarm, know how to quickly evacuate the building.
2. In case of fire, know the location of your fire extinguisher, and know how to activate the fire alarm.
3. In case of emergency, call 9-1-1.
4. In case of in intruder, call security or 9-1-1.

Your organization may provide you with detailed emergency procedures or manuals.



Good Computer Security Practices

- Every user of the USDA information systems has a responsibility to follow basic good security practices.
- As you review these practices, keep in mind that *your behavior sets the example for other employees*.

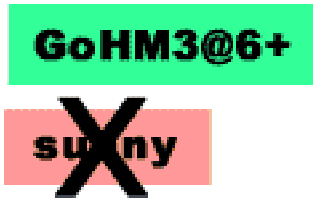
Good Computer Security Practices # 1

Never share your User ID and password!

Good Computer Security Practices # 2

Create strong passwords that are difficult to guess!

Combine upper and lower case letters with numbers and special characters.



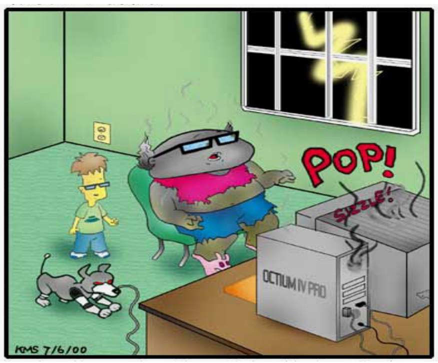
Good Computer Security Practices # 3

Do not leave your workstation unattended. Log off or Lockout your computer.

Use a screen saver that password protects your workstation when it is left unattended.

Good Computer Security Practices # 4

Backup your hard drive! Or save important files on your office server.



In a bitter twist of irony, Bob suddenly realized he had forgotten to save his 250 page article on "Preventive Maintenance: The Importance of Making Back-ups"

Good Computer Security Practices # 5

Keep food and drink away from your system and keyboard!

Good Computer Security Practices # 6

Limit personal use of your system and services such as e-mail and the Internet.

USDA DR-3300 provides guidance on personal use. Your organization may also have supplemental personal use policies.

Good Computer Security Practices # 7

Consider “Need to Know” before sharing information.

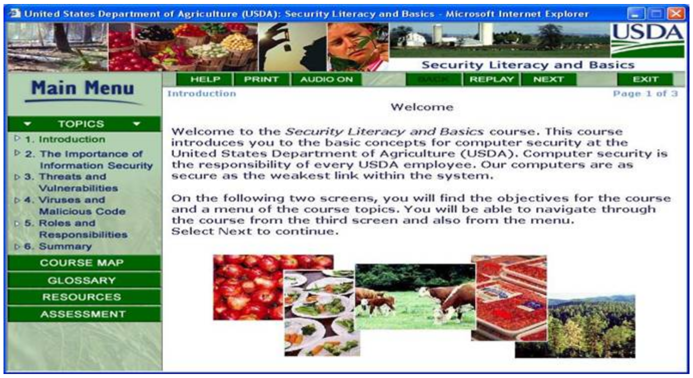
Good Computer Security Practices

USDA prohibits the following specific computer activities:

- The viewing or distribution of any pornographic material;
- Gambling;
- The use of government computers for Private Business activities;
- The installation of unauthorized software;
- Making Unauthorized Configuration changes;
- Online auctioning; and
- The downloading and use of Peer-to-Peer file sharing programs (e.g., Kazaa).

Security Literacy and Basics Course

You will be required to complete a Security Literacy and Basics Course on AgLearn within 60-90 days from receipt of your user ID. AgLearn can be accessed at: **www.aglearn.usda.gov**.


United States Department of Agriculture (USDA): Security Literacy and Basics - Microsoft Internet Explorer
USDA
Security Literacy and Basics
HELP
PRINT
AUDIO ON
BACK
REPLAY
NEXT
EXIT
Main Menu
TOPICS
1. Introduction
2. The Importance of Information Security
3. Threats and Vulnerabilities
4. Viruses and Malicious Code
5. Roles and Responsibilities
6. Summary
COURSE MAP
GLOSSARY
RESOURCES
ASSESSMENT
Introduction
Page 1 of 3

Welcome

Welcome to the *Security Literacy and Basics* course. This course introduces you to the basic concepts for computer security at the United States Department of Agriculture (USDA). Computer security is the responsibility of every USDA employee. Our computers are as secure as the weakest link within the system.

On the following two screens, you will find the objectives for the course and a menu of the course topics. You will be able to navigate through the course from the third screen and also from the menu. Select Next to continue.

Questions and Answers

For more information please call:

Craig Chase, Chief Security Policy Branch 202-690-0077 craig.chase@usda.gov

Janell Duke, Chief Security Operations Branch 816-926-1641 janell.duke@usda.gov

Greg Gage, ISSPM 202-720-8650 greg.gage@usda.gov